藤

NEWS LETTER

Ver. 2013. 05

TRAM SYSTEM

今月のコンテンツ

スマホリスク

ウィルス感染・・・？

シャドーITって・・・？

◎ これだけは知っておきたい スマホリスク

・スマホリスクはウィルスだけではない。

・企業利用する上での注意点

セキュアコンテナ・・・？

紛失・盗難の確率・・・？

カーネーション

5月の第2日曜日といえば「母の日」ですが、母の日の習慣は、アメリカで始まりました。アンナ・ジャービスという女性が、亡くなった母親のありがたさを実感し、母親のための祭日をつくって国中で祝うことを提案します。1908年（明治41年）の命日に最初の「母の日」として追悼会が行われ、参加者に母が好きだったカーネーションを配ったことから、カーネーションが母の日のシンボルになったようです。
ちなみに「黄色のカーネーション」の花言葉は「軽蔑」、「混色のカーネーション」は「愛の拒絶」なようです・・・。
わざわざそんな花言葉にせんでもという感じですよね・・・。

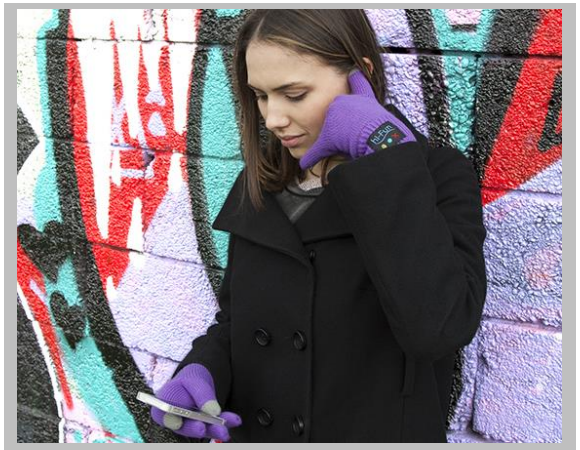
◎　これだけは知っておきたいスマホリスク

スマホリスクはウィルスだけではない

個人への普及が進み、企業利用でのケースも多くなってきたスマートホンですが、企業利用においてはセキュリティ面が気になるところですよね。
後追いにならないよう、漏れがないようにセキュリティ対策を講じてリスクを抑えていきましょう。

スマートホンのリスクと聞くと、ウィルスを思い浮かべる方が多いかと思います。
しかし、それはリスクの側面でしかなく、本質は企業情報の漏えいと流出にあるといえます。
間違った使い方や紛失などの事故も重大なリスクの要素となるわけです。

まずは情報漏えいや情報流出につながるリスクを網羅的に押さえていきます。
その上で、事前に回避できるもの、事後の対処方法などを把握し、セキュリティレベルを上げていきましょう。



親指がスピーカー、小指がマイクになっている手袋　冗談かと思ったらホントに売ってました・・。

スマホリスクの4大項目

① 紛失・盗難などの事故
② 悪質なアプリ・ウィルス
③ シャドーIT
④ ネットワークが関連するリスク

情報漏えいや情報流出につながるリスクで大別すると左記の4項目となり、この4項目さえ押さえていれば、スマホリスクはかなり軽減できます。
次ページから1項目ずつご説明していきますので、すでに企業利用されている方や、検討されている方はご参考にして頂ければと思います。

◎ これだけは知っておきたいスマホリスク

① 紛失・盗難などの事故

全ての企業で紛失・盗難の事故が起こると基本的に考えておくべきです。
社外で使うことが多いスマートホンは、置忘れや盗まれるケースが後を絶ちません。
日本ネットワークセキュリティ協会の調査結果によると、1年におよそ100人に2人の割合で紛失・盗難に逢っているそうです。
もはや携帯電話は紛失するものとして対策を準備しておく必要があります。
紛失してからの対策と手順を右にご紹介しますので参考にして下さい。

② 悪質なアプリ・ウィルス

先月号でもご紹介しましたが、スマホを狙うウィルスのほとんどがAndroid端末向けです。2012年はAndroidを狙ったものが9割を超えるそうです。
対策としては、実績のあるウィルス対策ソフトの導入と、不用意なインストールは極力避けることが最も重要です。
また、コンシューマー向けの無料通話やSNSのアプリのなかには、アドレス帳のエントリーをサービス側のサーバーに送信することが可能なものがあります。取引先の連絡先をアドレス帳に登録した後でこうしたアプリを使い始めると、業務データが自社の管理の及ばないところに送られてしまうので、インストールする際には注意が必要です。

スマホを無くした！！

▼

① 企業の管理者（②～⑤を実施する人）へ連絡

▼

② スマホの位置情報を取得して探す

アプリやキャリアサービスでスマホが現在何処にあるのかがすぐに分かるものがあります。

▼

③ 遠隔でワイプをかける

遠隔からスマホに命令をだし端末内のデータを消去できる「リモートワイプ」を利用しましょう。

▼

④ 電話を止める（回線停止）

通信と通話を使えなくします。ワイプの前に止めてしまうとワイプの成功率が低くなるので注意です。

▼

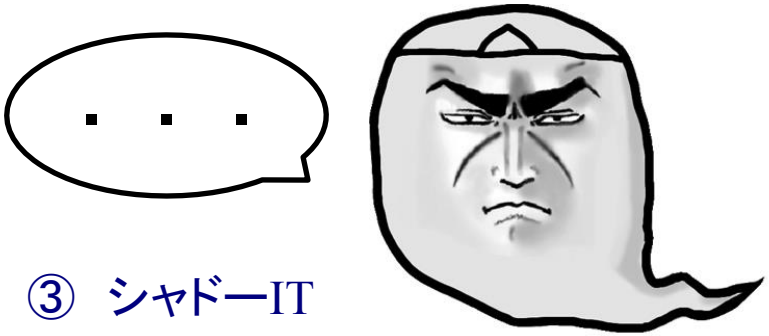
⑤ 社内アクセス権限の失効

紛失したスマホに割り当てられた社内アクセス権限を失効させ、wifi等から入られないようにします。

▼

⑥ 警察に届け出る

◎ これだけは知っておきたいスマホリスク



③ シャドーIT

「シャドーIT」とは、企業が管理できていない状態のIT製品やサービスを業務に利用する事を指します。
【例】 会社が管理出来ていない状況で、「SNSなどで顧客とやり取りをする」「会社のメールを外部のサービスに転送して見る」「アドレス帳に顧客の連絡先を登録する」などが挙げられます。社内データを抱えたまま紛失・盗難に合えば、①に挙げた対策も警察の届出くらいしかできません。ウィルス対策やアプリの選択も個人の裁量になる上に、事が起こった時に原因を追究しにくくなりますので注意が必要です。

④ ネットワークが関連するリスク

スマホはPCとほぼ同程度のネットワーク接続機能がある上、VPNクライアントを搭載しています。これを従業員が勝手に社内ネットワークに繋いでしまう可能性もあるのです。
マイパソコンの持ち込みを禁止している企業や、社内ルールの範囲内でのみ使用を許可するという企業が多いと思いますが、個人携帯にはそれほど注目していないのが実情です。しかし、スマホはもはやパソコンなのです、「マイパソコンを持ち込んでいるんだ」という認識を企業・従業員とも忘れてはいけません。

今回ご紹介致しました4項目は、あくまで「現時点」でのリスクと対策です。
目まぐるしいスピードで進歩しているスマートホン、常に新しい情報を仕入れられる環境こそが、最も重要なセキュリティ対策と言えるかもしれません。

TRAM SYSTEM

トラムシステム株式会社
〒465-0063
愛知県名古屋市名東区新宿2丁目55番地
TEL:052-701-2634
FAX:052-701-2637
Mail：info@tramsystem.jp